

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Fredrik Lindholm

Application No 10/552,955

Filed: 10/14/2005

Attorney Docket No: P18053-US1
Customer No.: 27045

For: Authentication Method

§ Group Art Unit: 2436

§

§ Examiner: Nguyen, Trong H

§

§ Confirmation No: 2497

§

Via EFS-Web

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313.1450

CERTIFICATE OF TRANSMISSION BY EFS-WEB

Date of Transmission: _January 26, 2011

I hereby certify that this paper or fee is being transmitted to the United States Patent and Trademark Office electronically via EFS-Web.

Type or Print Name: Jennifer Hardin

_____/Jennifer Hardin/_____

APPLICANT'S REPLY BRIEF FILED UNDER 37 C.F.R. §1.193(b)(1)

In response to the Examiner's Answer having a mail date of November 26, 2010, the Applicants submit this reply brief.

Arguments

1.) CLAIMS 1-11 and 13-24 ARE DIRECTED TO STATUTORY SUBJECT MATTER

In response to Applicant's arguments traversing the rejection of claims 1-11 and 13-24 as being directed to non-statutory subject matter, the Examiner states that:

" . . . those claims fail the machine or transformation test as the steps recited . . . could be performed in one's mind or manually without any apparatus. It should be noted that [the] claims [recite] steps being performed 'at' the first or second unit which could be reasonably interpreted as being performed 'near' or 'on' the first or second unit."
[emphasis added]

The Examiner's interpretation of the claims is not reasonable. First, claim 1 clearly recites the method is performed "in a communication system including at least two units." (emphasis added) Furthermore, claim 1 recites the step of "determining, at a first unit, a check token for a second unit based on [a] password inputted by a user of said first unit . . ." (emphasis added) What does the user "input" the password to, if not the first unit? If the user could determine a check token based on the password purely by a mental process, there would be no reason to bother with inputting the password into anything. Thus, the Examiner's interpretation of the claims is unreasonable, as it would require reading explicit limitations out of the claims. Therefore, the rejection of claims 1-11 and 13-24 as being directed to non-statutory subject matter should be reversed.

2.) CLAIMS 1, 10, 11, 13, 15-21, 23, 25, 32, 34-41 AND 45 ARE NOT ANTICIPATED BY U.S. PATENT NO. 6,792,533 ("JABLON")

In responding to Applicant's arguments, the Examiner asserts that certain features upon which Applicant's arguments were based are not recited in the claims; *i.e.*, that "individualized" means "unique." The Examiner supports his opinion by asserting that claim terms must be given their broadest reasonable interpretation, and that he has interpreted "individual" to mean that "each unit individually possesses a copy of an item." The Examiner's interpretation is not reasonable.

Claim 1 recites:

1. A method for password-based authentication in a communication system including a group of at least two units associated with a common password, comprising the steps of;

assigning individual authentication tokens to the respective units in the group based on the password such that each authentication token is irreversibly determined by the password;

determining, at a first unit, a check token for a second unit based on the password inputted by a user of said first unit and the authentication token of the first unit, wherein the step of determining the check token comprises the steps of;

determining, at the first unit, a token secret using the authentication token of the first unit and the password; and,

creating, at the first unit, the check token for the second unit based on the token secret and the password;

sending the check token to the second unit; and,

comparing, at the second unit, the check token with the authentication token of the second unit for authentication of the first unit towards the second unit, *wherein said user of said first unit is authenticated if said check token is the same as said authentication token of said second unit*. (emphasis added)

The claimed invention is characterized by individual *authentication* tokens, assigned to units in a group of at least two units associated with a common password, that are irreversibly determined by a password. A password inputted by a user of a first unit and an authentication token of the first unit are used to determine a *check* token for a second unit. This is accomplished by first determining, at the first unit, a token secret using the authentication token **of the first unit** and the inputted password; the *check* token **for the second unit** is then created based on the token secret and the password. The *check* token is then sent to the second unit where it is compared with the *authentication* token **of the second unit**; if they are the same, then the user of the first device is considered authenticated.

The Examiner's arguments are based on a claim interpretation that "individual" means that "each unit individually possesses a copy of an item," which implies that the check tokens of the first and second units are the same, as opposed to being "unique" as argued by Applicant. That interpretation is unreasonable when the limitations of the claim are viewed as a whole.

First, claim 1 states that individual authentication tokens are assigned to the respective units. If the claim only required "a" single authentication token for all units, then the word "individual" would be superfluous and "tokens" would be an improper plural; *i.e.*, the claim would instead recite "assigning an authentication token to the respective units.

Secondly, as recited in claim 1, a check token for a second unit is determined **at a first unit** based, in part, on the authentication token **of the first unit**. Subsequently, the check token for the second unit (as determined at the first unit) is sent to the second unit. The second unit then compares the received check token with the authentication token **of the second unit**, wherein *the user of the first unit is authenticated if the check token is the same as the authentication token of the second unit*. If the Examiner's interpretation of "individual" was reasonable, there would be no reason to

transmit a check token from the first unit to the second unit, since it is a function of a password inputted by a user of the first unit and the authentication token of the first unit, which the Examiner's interpretation requires to be the same as the authentication token of the second unit. In other words, if the units shared the same authentication token, then why determine a check token that is a function of the authentication token and the user's password? If the authentication tokens of the various units are all the same, then the check token would only vary as a function of the user's password. According to claim 1, however, the check token is a function of not only the user's password, but the authentication token of that user's device (e.g., the first unit).

Finally, the Examiner asserts that the Applicant's specification does not specifically define "individual," and that under the broadest reasonable interpretation consistent with the specification, the Examiner can interpret "individual" to mean that "each unit individually possesses a copy of an item." The Examiner's interpretation, however, is not consistent with the Applicant's specification. At page 8, line 20, it is described how a first unit ("device i") uses a combination of "its own authentication token R_i " and the user's password (P) to unlock (*i.e.*, determine) a token secret (S). It is then described how the first unit ("device i") uses S and P to create a check token (M_j) for a second unit ("device j"). The check token M_j represents the authentication token "that should be available at device j if the user has input the correct password. The check token (M_j) is then sent to the second unit (device j) where it is compared with "the actual authentication token R_j " of the second unit (device j). Thus, the Applicant's specification describes how the first unit has its own authentication token R_i , while the second unit has its own authentication token R_j ; *i.e.*, R_i and R_j represent the individual and unique authentication tokens of the first and second units, respectively. Accordingly, the Examiner's interpretation of that claim limitation is not consistent with Applicant's specification. Therefore, for the reasons presented in Applicant's Appeal Brief, it is respectfully requested that the Examiner's rejection of claims 1, 10, 11, 13, 15-21, 23, 25, 32, 34-41 and 45 be reversed.

3.) CLAIMS 2, 26 AND 42 ARE PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 6,721,886 ("USKELA")

The Examiner rejected claims 2, 26 and 42 as being unpatentable over Jablon in view of U.S. Patent No. 6,721,886 ("Uskela"). As established *supra*, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 2, 26 and 42 are dependent, respectively. The Examiner has not pointed to any teaching in Uskela to overcome the deficiency in the teachings of Jablon and, therefore, claims 2, 26 and 42 are not obvious in view of that combination of references.

4.) CLAIMS 3, 5, 27, 29 AND 43 ARE PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 5,778,066 ("HAUSER")

The Examiner rejected claims 3, 5, 27, 29 and 43 as being unpatentable over Jablon in view of U.S. Patent No. 5,778,066 ("Hauser"). As established *supra*, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 3, 5, 27, 29 and 43 are dependent. The Examiner has not pointed to any teaching in Hauser to overcome the deficiency in the teachings of Jablon and, therefore, claims 3, 5, 27, 29 and 43 are not obvious in view of that combination of references.

5.) CLAIMS 4 AND 28 ARE PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,397,329 ("AIELIO")

The Examiner rejected claims 4 and 28 as being unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,397,329 ("Aielio"). As established *supra*, Jablon fails to anticipate independent claims 1 and 25, from which claims 4 and 28 are dependent, respectively. The Examiner has not pointed to any teaching in Aielio to overcome the deficiency in the teachings of Jablon and, therefore, claims 4 and 28 are not obvious in view of that combination of references.

6.) CLAIMS 7, 8, 31 AND 44 ARE PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,215,877 ("MATSUMOTO")

The Examiner rejected claims 7, 8, 31 and 44 as being unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,215,877 ("Matsumoto"). As established *supra*, Jablon fails to anticipate independent claims 1, 25 and 41, from which claims 7, 8, 31 and 44 are dependent. The Examiner has not pointed to any teaching in Matsumoto to overcome the deficiency in the teachings of Jablon and, therefore, claims 7, 8, 31 and 44 are not obvious in view of that combination of references.

7.) CLAIM 9 IS PATENTABLE OVER JABLON IN VIEW HAUSER, MATSUMOTO AND U.S. PATENT NO. 6,885,388 ("GUNTER")

The Examiner rejected claim 9 as being unpatentable over Jablon in view Hauser, Matsumoto and U.S. Patent No. 6,885,388 ("Gunter"). As established *supra*, Jablon fails to anticipate independent claim 1, from which claim 9 is dependent. The Examiner has not pointed to any teaching in Gunter to overcome the deficiency in the teachings of Jablon and, therefore, claim 9 is not obvious in view of that combination of references.

8.) CLAIM 14 IS UNPATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 7,363,494 ("BRAINARD")

The Examiner rejected claim 14 as being unpatentable over Jablon in view of U.S. Patent No. 7,363,494 ("Brainard"). As established *supra*, Jablon fails to anticipate independent claim 1, from which claim 14 is dependent. The Examiner has not pointed to any teaching in Brainard to overcome the deficiency in the teachings of Jablon and, therefore, claim 14 is not obvious in view of that combination of references.

9.) CLAIM 22 IS PATENTABLE OVER JABLON IN VIEW OF HAUSER AND U.S. PATENT NO. 6,668,167 ("MCDOWELL")

The Examiner rejected claim 22 as being unpatentable over Jablon in view of Hauser and U.S. Patent No. 6,668,167 ("McDowell"). As established *supra*, Jablon fails

to anticipate independent claim 1, from which claim 22 is dependent. The Examiner has not pointed to any teaching in McDowell to overcome the deficiency in the teachings of Jablon and, therefore, claim 22 is not obvious in view of that combination of references.

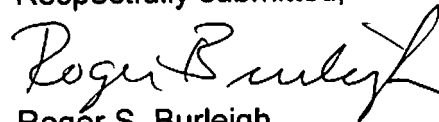
10.) CLAIM 24 IS PATENTABLE OVER JABLON IN VIEW OF U.S. PATENT NO. 7,076,656 ("MACKENZIE")

The Examiner rejected claim 24 as being unpatentable over Jablon in view of U.S. Patent No. 7,076,656 ("MacKenzie"). As established *supra*, Jablon fails to anticipate independent claim 1, from which claim 24 is dependent. The Examiner has not pointed to any teaching in MacKenzie to overcome the deficiency in the teachings of Jablon and, therefore, claim 24 is not obvious in view of that combination of references.

CONCLUSION

As established by the arguments in Applicant's Appeal Brief, and further elaborated herein in response to the Examiner's Answer, claims 1-11, 13-32 and 34-45 are patentable over the prior art of record, and the Applicant requests that the rejections thereof be reversed and the application be remanded for further prosecution.

Respectfully submitted,



Roger S. Burleigh
Registration No. 40,542
Ericsson Patent Counsel

Date: January 26, 2011

Ericsson Inc.
6300 Legacy Drive, M/S EVR1 C-11
Plano, Texas 75024

(972) 583-5799
roger.burleigh@ericsson.com